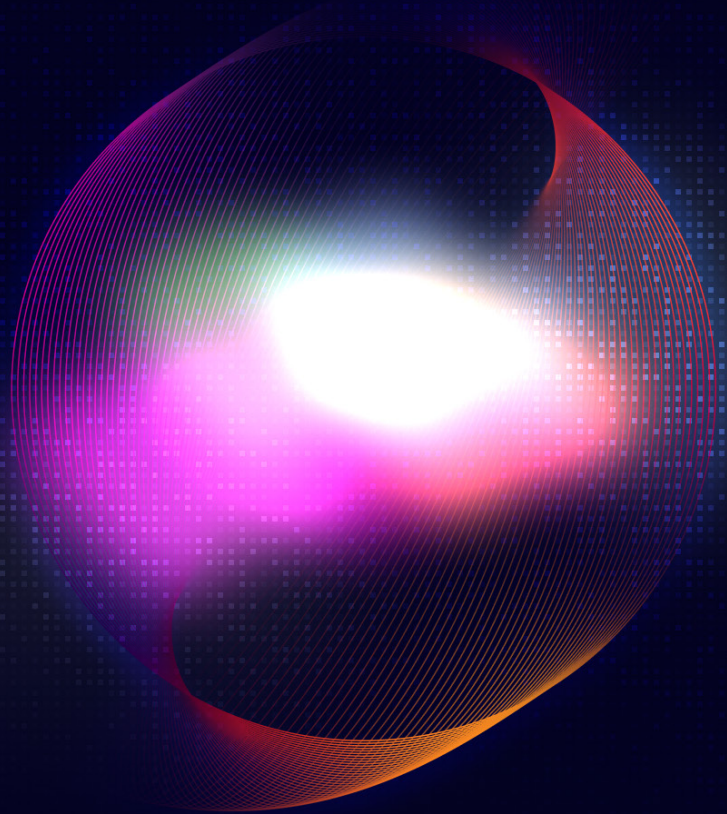




Unified IT/OT Security

Part of the Exclusive Networks OT
Security Center of Excellence



FORTINET® +  **NOZOMI
NETWORKS**

As operational technology becomes increasingly connected, and increasingly targeted, organizations must secure both IT and OT infrastructure without adding complexity. The convergence of Information Technology (IT) and Operational Technology (OT), now widely recognized as Cyber-Physical Systems (CPS) by Gartner, creates both opportunity and risk.






Here's how Exclusive Networks' integrated approach combines Fortinet's Security Fabric with Nozomi Networks' OT visibility platform to deliver comprehensive Cyber-Physical System Protection Platform (CPSPP) capabilities across the entire Purdue Model.

THE CHALLENGE

Bridging the IT/OT Security Gap

Legacy Systems Meet Modern Threats

Legacy OT systems weren't designed for connectivity, but they're now prime targets for sophisticated attacks. Organizations operating Industrial Control Systems (ICS) in critical infrastructure face:

-  **Expanding Attack Surface:** IT/OT convergence creates new vulnerabilities across previously isolated systems
-  **Operational Continuity Requirements:** In OT environments, availability often trumps confidentiality—security solutions must maintain uptime and safety
-  **Limited OT Protocol Visibility:** Traditional IT security tools lack visibility into specialized protocols like Modbus, DNP3, and EtherNet/IP
-  **Regulatory Pressure:** Increasing compliance requirements (NERC CIP, TSA directives, sector-specific mandates) demand integrated cybersecurity approaches
-  **Skills Shortage:** Organizations struggle to find professionals who understand both IT security and OT operations

The Siloed Approach Leaves Dangerous Gaps

When IT and OT security remain separate, organizations face incomplete visibility, inconsistent policy enforcement, and slower incident response. The critical security boundary between enterprise networks and industrial control systems requires unified protection.

THE SOLUTION

Fortinet Security Fabric + Nozomi Networks

Integrated Architecture for Complete Coverage

The combined Fortinet and Nozomi Networks solution provides end-to-end protection across all Purdue Model levels, from field devices to enterprise networks.



OT Visibility and Threat Detection

Nozomi Networks delivers comprehensive asset discovery and behavioral analytics purpose-built for operational technology environments.



Gartner Recognition: Nozomi Networks is recognized as a Leader in Gartner's 2025 Magic Quadrant for Cyber-Physical System Protection Platforms.

Key Capabilities:

- **Asset Visibility:** Automatic discovery and inventory of all OT assets, including PLCs, SCADA systems, ICS controllers, and IoT devices
- **OT Protocol Analysis:** Deep packet inspection of industrial protocols (Modbus, DNP3, EtherNet/IP, BACnet, and more)
- **Behavioral Analytics:** AI-driven anomaly detection that identifies threats without disrupting operations
- **Threat Intelligence:** Real-time alerts on vulnerabilities, configuration changes, and suspicious activities
- **Compliance Reporting:** Automated compliance mapping for NERC CIP, IEC 62443, and other frameworks



Fortinet Security Fabric: Unified IT/OT Security

Fortinet provides integrated security across the entire infrastructure through its Security Fabric architecture.



Analyst recognition: Fortinet is consistently recognized as the overall leader in the annual Westlands Advisory IT/OT Network Protection Platform Navigator report.

Key Capabilities:

- **Next-Generation Firewalls:** Purpose-built FortiGate appliances for OT environments with industrial protocol support
- **Network Access Control:** FortiNAC for device visibility and policy enforcement across IT and OT networks
- **Secure Segmentation:** Microsegmentation capabilities that isolate critical OT assets while maintaining operational workflows
- **Zero Trust Implementation:** Unified policy enforcement from enterprise to control room
- **Secure SD-WAN:** FortiGate SD-WAN for distributed OT/IT sites with built-in security

Purdue Model Integration

Levels 0–2 Process, Basic Control, Supervisory Control	<ul style="list-style-type: none">• Nozomi Networks provides passive monitoring and asset discovery• Fortinet FortiGate appliances enforce security policies without impacting real-time operations• Combined visibility into field devices, SCADA systems, and HMI platforms
Level 3 Operations Management	<ul style="list-style-type: none">• Critical DMZ boundary with Fortinet Security Fabric integration• Nozomi threat detection feeds into Fortinet’s unified security management• Microsegmentation protects MES and production systems
Levels 4–5 Business Logistics, Enterprise Network	<ul style="list-style-type: none">• Fortinet Security Fabric extends from OT through IT infrastructure• Unified policy enforcement across converged environments• Integration with existing IT security tools and workflows

Use Cases



Manufacturing & Industrial Automation

Challenge: High OT system exposure with growing IoT integration

Solution: Nozomi discovers all connected assets while Fortinet secures smart factory connectivity

Outcome: Complete visibility and protection for Industry 4.0 initiatives



Energy & Utilities

Challenge: Critical infrastructure with strict NERC CIP compliance requirements

Solution: Automated compliance reporting from Nozomi plus Zero Trust enforcement from Fortinet

Outcome: Regulatory alignment with proactive threat defense



Transportation & Logistics

Challenge: Interconnected systems across distributed physical infrastructure

Solution: Fortinet Secure SD-WAN with Nozomi monitoring for rail, ports, and fleet systems

Outcome: Secure connectivity with operational visibility across all sites

Key Benefits



Unified Visibility from Enterprise to Control Room

Achieve end-to-end situational awareness across IT and OT environments. Nozomi delivers asset discovery and anomaly detection while Fortinet enforces unified Zero Trust policies.



Operational Continuity Without Compromise

Purpose-built solutions maintain uptime and safety requirements. Passive monitoring and non-disruptive security controls protect operations while defending against threats.



Regulatory Compliance Made Simple

Automated compliance mapping aligns with NERC CIP, IEC 62443, ISA/IEC standards, NIST CSF, and sector-specific mandates. Pre-validated architectures accelerate audit readiness.



Faster Threat Detection and Response

Integrated threat intelligence flows between Nozomi's behavioral analytics and Fortinet's Security Fabric, enabling rapid response to OT-specific threats.



Scalable Multi-Vendor Integration

Exclusive Networks' aggregation model extends beyond Fortinet and Nozomi to include complementary solutions like SentinelOne for endpoint protection, Netskope for cloud security, and Juniper, Ruckus and Meter for resilient networking.

Through the Exclusive Networks OT Security Center of Excellence, we help organizations Protect What's Next — delivering the visibility, resilience, and compliance needed to secure cyber-physical systems across manufacturing, energy, transportation, and critical infrastructure.

WHY EXCLUSIVE NETWORKS?

The Trusted Global Cybersecurity Specialist

Exclusive Networks is uniquely positioned as a global trusted cybersecurity specialist to bridge the IT/OT divide by enabling secure CPS transformation. Through our ecosystem of best-in-class CPS Protection Platforms and services, we help organizations achieve resilience, regulatory alignment, and innovation at scale.

OT Security Center of Excellence

Our comprehensive approach delivers tangible value through:

- Business Development Resources: Dedicated OT Security Practice Managers
- Technical Resources: Pre-sales Engineers with OT security certifications
- Best-in-Class Vendor Portfolio: Fortinet, Nozomi Networks, and other industry leaders
- Integrated Partner Enablement: Multi-faceted campaigns and enablement programs
- Industry-Specific Demand Generation: Targeted capabilities across key verticals

Services-Led Aggregation Model

We simplify complexity by integrating complementary vendor solutions into pre-validated architectures and delivering scalable, partner-ready tailored services via Cloudrise that simplify IT/OT security deployment and operations.

This solution is a core component of the Exclusive Networks OT Security Center of Excellence — uniting vendors, partners, and customers to protect what's next across the cyber-physical ecosystem.